ADVANCES IN APPLIED MATHEMATICS 4, 175–196 (1983)

The Mathematics of Perfect Shuffles

PERSI DIACONIS

Stanford University, Stanford, California 94305 and Harvard University, Cambridge, Massachusetts 02138

R. L. GRAHAM

Bell Laboratories, Murray Hill, New Jersey 07974 and Stanford University, Stanford, California 94305

WILLIAM M. KANTOR

University of Oregon, Eugene, Oregon 97403 and Bell Laboratories, Murray Hill, New Jersey 07974

There are two ways to perfectly shuffle a deck of $2n$ cards. Both methods cut the deck in half and interlace perfectly. The out shuffle O leaves the original top card on top. The in shuffle I leaves the original top card second from the top. Applications to the design of computer networks and card tricks are reviewed. The main result is the determination of the group $\langle I, O\rangle$ generated by the two shuffles, for all n. If $2n$ is not a power of 2, and if $2n \neq 12, 24$, then $\langle I, O\rangle$ has index 1, 2, or 4 in the Weyl group B_n (the group of all $2^n n!$ signed $n \times n$ permutation matrices). If $2n = 2^k$, then $\langle I, O\rangle$ is isomorphic to a semi-direct product of Z_2^k and Z_k. When $2n = 24$, $\langle I, O\rangle$ is isomorphic to a semi-direct product of Z_2^{11} and M_{12}, the Mathieu group of degree 12. When $2n = 12$, $\langle I, O\rangle$ is isomorphic to a semi-direct product of Z_2^6 and the group $PGL(2, 5)$ of all linear fractional transformations over $GF(5)$.

1. INTRODUCTION

There are two ways to perfectly shuffle a deck of $2n$ cards. Both cut the deck in half and interlace perfectly. The *in* shuffle I leaves the original top card second from the top. The *out* shuffle O leaves the original top card on top. Let the deck be labeled $(0, 1, \ldots, n-1, n, \ldots, 2n-1)$. After an in shuffle the order is $(n, 0, n+1, \ldots, 2n-1, n-1)$. After an out shuffle, the order is $(0, n, 1, n+1, \ldots, n-1, 2n-1)$. These shuffles have been used by gamblers and magicians to manipulate cards. A historical review,

0196-8858/83 $7.50

describing "widely known" properties of the shuffles, is in Section 3. This section also describes results of Levy on the cycle structure of the shuffles, and results concerning decks of odd size.

In and out shuffles appear in computer science as a way of connecting processors in parallel processing machines. One widely known application is an $O(\log n)$ FFT algorithm. Section 4 discusses these applications as well as some new results; for example, an array of 2^k numbers can be reversed in k in shuffles. Section 5 discusses some related permutations: Levy's work on the "milk shuffle" and Morris' work on generalized perfect shuffles.

The main result of this paper is a determination of the group generated by in and out shuffles. This group will be called the shuffle group and denoted $\langle I, O\rangle$. Both of the generators I and O preserve central symmetry; that is, cards symmetrically located about the center of the deck (0 and $2n-1$, 1 and $2n-2$, etc.) are sent to positions symmetric about the center. Thus $\langle I, O\rangle$ is a subgroup of the centrally symmetric permutations. This group is isomorphic to the Weyl group B_n of $n \times n$ signed permutation matrices. This is the group of all $n \times n$ matrices with entries $0, \pm 1$, and one nonzero entry in every row and column. Equivalently, it is the group of all $2^n n!$ symmetries of the n-dimensional generalization of the octahedron, whose vertices are $\pm e_1, \ldots, \pm e_n$, where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$ (see Coxeter [5]). The pairs $\{e_i, -e_i\}$ correspond to the pairs of card positions which are centrally symmetric.

We will have to deal with three homomorphisms of B_n. If $g \in B_n$ then $\operatorname{sgn}(g)$ is its sign as a permutation of $2n$ cards, and $\overline{\operatorname{sgn}}(g)$ is its sign as a permutation of n centrally symmetric pairs; and $g \to \operatorname{sgn}(g)\overline{\operatorname{sgn}}(g)$ is a further homomorphism to $\{\pm 1\}$, whose kernel is the Weyl group D_n.

THEOREM. *Let $\langle I, O\rangle$ be the permutation group generated by in and out shuffles of $2n$ cards.*

(a) *If $n \equiv 2 \pmod 4$ and $n > 6$, then $\langle I, O\rangle$ is isomorphic to B_n and $|\langle I, O\rangle| = n!2^n$. If $n = 6$, then $\langle I, O\rangle$ is a semi-direct product of Z_2^6 with $PGL(2, 5)$.*

(b) *If $n \equiv 1 \pmod 4$ and $n \geqslant 5$, then $\langle I, O\rangle$ is the kernel of $\overline{\operatorname{sgn}}$ and $|\langle I, O\rangle| = n!2^{n-1}$.*

(c) *If $n \equiv 3 \pmod 4$, then $\langle I, O\rangle$ is isomorphic to D_n and $|\langle I, O\rangle| = n!2^{n-1}$.*

(d) *If $n \equiv 0 \pmod 4$, $n > 12$, and n not a power of 2, then $\langle I, O\rangle$ is the intersection of the kernels of sgn and $\overline{\operatorname{sgn}}$, and $|\langle I, O\rangle| = n!2^{n-2}$. If $2n = 24$, then $\langle I, O\rangle$ is a semi-direct product of Z_2^{11} with the Mathieu group M_{12} of degree 12.*

(e) *If $2n = 2^k$, $\langle I, O\rangle$ is isomorphic to the semi-direct product of Z_2^k by Z_k, where Z_k acts by a cyclic shift and $|\langle I, O\rangle| = k \cdot 2^k$.*

TABLE I
Order of the Group $\langle I, O \rangle$; $M = 2^n n!$

$2n$	2	4	6	8	10	12	14	16	18
$\lvert\langle I, O\rangle\rvert$	2	$2 \cdot 2^2$	$M/2$	$3 \cdot 2^3$	$M/2$	$M/3!$	$M/2$	$4 \cdot 2^4$	$M/2$
$2n$	20	22	24	26	28	30	32	34	36
$\lvert\langle I, O\rangle\rvert$	M	$M/2$	$M/(7! \cdot 2)$	$M/2$	M	$M/2$	$5 \cdot 2^5$	$M/2$	M
$2n$	38	40	42	44	46	48	50	52	
$\lvert\langle I, O\rangle\rvert$	$M/2$	$M/4$	$M/2$	M	$M/2$	$M/4$	$M/2$	M	

The theorem, and a number of other results about the shuffle group, are proved in Section 2. A list of the order of the shuffle group for $2n = 2, 4, \ldots, 52$, appears in Table I. This table was computed using a streamlined implementation of an algorithm of Sims [24] developed by Eric Hamilton and Donald Knuth at Stanford University. The numerical evidence allowed us to guess at the theorem. For a discussion of Sims' algorithm see Furst *et al.* [7].

Finally, we mention the connection between our shuffles (for a deck of 24 cards) and some very recent work of Borcherds *et al.* [2] on representations of the Leech lattice in hyperbolic space. Section 5 contains further discussion.

2. Proof of the Theorem

We begin by establishing a number of basic properties of perfect shuffles. Lemma 1 gives the order of in and out shuffles. It is well known: see Uspensky and Heaslet [26, pp. 244–245], Herstein and Kaplansky [11, Chap. 3.4].

Lemma 1. *The order of the in shuffle permutation is the order of* 2 $(\mathrm{mod}\, 2n + 1)$. *The order of the out shuffle is the order of* 2 $(\mathrm{mod}\, 2n - 1)$.

Proof. The order of an in shuffle is the order of an out shuffle with a deck containing 2 more cards, so we only prove the result for out shuffles. If the deck is labeled $0, 1, \ldots, 2n - 1$, then after one out shuffle the card labeled j is at position $2j \pmod{2n - 1}$ if $j < 2n - 1$. After k shuffles it is in position $2^k j \pmod{2n - 1}$. All cards will be in their original positions for the smallest k such that $2^k \equiv 1 \pmod{2n - 1}$. □

Remark. A pack of 52 cards requires 8 out shuffles or 52 in shuffles to recycle. Because of Fermat's theorem, the pack will always recycle after

at most $2n - 2$ out shuffles, although fewer may do. A famous conjecture of Artin asserts that 2 is a primitive root (mod p) for infinitely many primes p. If this is true, there are arbitrarily large n such that $2n - 2$ out shuffles are required to recycle $2n$ cards.

Lemma 2 gives an algorithm for bringing the top card to any position by a sequence of in and out shuffles. The result was first given by Alex Elmsley. For a proof, see Morris [21, Proposition 1].

LEMMA 2. *Let the positions in a deck of* $2n$ *cards be labeled* $0, 1, \ldots, 2n - 1$. *To bring the top card to position* k, *express* k *in binary, interpret* 1 *as in and* 0 *as out, and perform the indicated sequence of in and out shuffles from left to right.*

Lemmas 1 and 2 give the following lower bound for the shuffle group:

LEMMA 3. *The order of the shuffle group is at least* $2n \times$ *order of* 2 $(\text{mod } 2n - 1)$.

The next result proves part (d) of the theorem. It establishes that the lower bound of Lemma 3 is achieved for decks of size 2^k. The proof provides a simple interpretation of in and out shuffles as maps on the vector space Z_2^k.

LEMMA 4. *For* $2n = 2^k$, *the shuffle group is isomorphic to a semi-direct product of* Z_2^k *by* Z_k.

Proof. Label the cards using their binary expansions $(x_1, \ldots, x_k)$. It is easy to check that, using an obvious notation,

$$O: \quad (x_1, x_2, \ldots, x_k) \to (x_2, x_3, \ldots, x_k, x_1),$$
$$I: \quad (x_1, x_2, \ldots, x_k) \to (x_2, x_3, \ldots, x_k, \bar{x}_1) \qquad \text{with } \bar{x}_1 = 1 - x_1.$$

The permutations O^j, $0 \leqslant j < k$, form a cyclic group $\langle O \rangle$. The permutations $B_j = O^{j-1} I O^{-j}$ send $(x_1, \ldots, x_j, \ldots, x_k)$ into $(x_1, \ldots, \bar{x}_j, \ldots, x_k)$, for $1 \leqslant j \leqslant k$. Map Z_2^k into the shuffle group by sending $a = (a_1, \ldots, a_k) \in Z_2^k$ into $\prod_{j=1}^{k} B_j^{a_j}$. It is easy to see this is an isomorphism. The image group intersects the cyclic group $\langle O \rangle$ only in the identity and their product contains O and I. The action of Z_k on Z_2^k is a cyclic shift. □

Both in and out shuffles preserve arrangements with "central symmetry." We now turn to definitions and amplification of this fact. Throughout, permutations will be applied on the right, so xg is the image of x under the permutation g. S_n and A_n denote the symmetric and alternating groups of degree n. If S is a set of permutations, then $\langle S \rangle$ denotes the group generated by S.

DEFINITIONS. If $a < b$, then $[a, b) = \{x \in Z | a \leqslant x < b\}$. A permutation $g \in S_{2n}$ has *central symmetry* if $(i)g + (2n - 1 - i)g = 2n - 1$ for all $i \in [0, n)$. The subgroup of centrally symmetric permutations is denoted B_n. It is natural to label the objects being permuted as $0, 1, \ldots, n-1, (n-1)', \ldots, 1', 0'$, where $x \leftrightarrow x'$ is the natural pairing. Let $\bar{x} = \{x, x'\}$. A permutation $g \in B_n$ induces a permutation $\bar{g}$ of $\{\bar{x} | x \in [0, n)\}$. The map $g \to \bar{g}$ is a homomorphism from B_n onto S_n with kernel equal to $\langle (0,0') \rangle \times \langle (1,1') \rangle \times \cdots \times \langle (n-1,(n-1)') \rangle \cong Z_2^n$. Note that $\operatorname{sgn}(g) = \operatorname{sgn}(\bar{g})$.

In this notation the shuffles can be written

$$O: \begin{cases} x \to 2x & \text{and } x' \to (2x)', & \text{if } x \in [0, \tfrac{1}{2}n), \\ x \to (2(n-x)-1)' & \text{and } x' \to 2(n-x)-1, & \text{if } x \in [\tfrac{1}{2}n, n); \end{cases}$$

$$I: \begin{cases} x \to 2x+1 & \text{and } x' \to (2x+1)', & \text{if } x \in [0, (n-1)/2), \\ x \to (2(n-x-1))' & \text{and } x' \to 2(n-x-1), & \text{if } x \in [(n-1)/2, n). \end{cases}$$

Let $G = \langle I, O \rangle$. Let $\bar{G}$ be the image of G in S_n and let K be the kernel of $G \to \bar{G}$.

LEMMA 5. *When $n = 12$, $\bar{G}$ is isomorphic to M_{12} and K is isomorphic to Z_2^{11}.*

Proof. The group $\bar{G}$ is generated by $\bar{O} = (\bar{1}\bar{2}\bar{4}\bar{8}\bar{7}\bar{9}\bar{5}\bar{1}\bar{0}\bar{3}\bar{6}\bar{1}\bar{1})$ and $\bar{I} = (\bar{0}\bar{1}\bar{3}\bar{7}\bar{8}\bar{6}\bar{1}\bar{0}\bar{2}\bar{5}\bar{1}\bar{1})(\bar{4}\bar{9})$. A computer check shows that the order of $\bar{G}$ is 95,040, the order of M_{12}. Further, $\bar{G}$ is doubly transitive; indeed $\bar{O}$ is an 11-cycle fixing $\bar{O}$ and $\bar{I}$ moves $\bar{O}$, so $\bar{G}$ is transitive, and to bring symbols labeled (i, j) to positions (k, l), bring i to 0, bring j to the appropriate place by iterates of $\bar{O}$, and then bring i to k. Sims [24] showed that M_{12} is the only doubly transitive permutation group of this order. The result for K follows from the order of G given in Table I. □

We were intrigued by the appearance of M_{12}. Table II lists 66 6-sets; these sets and their complements in [0, 12) form the design $S(5, 6, 12)$: each 5-set is in exactly one of the 132 6-sets. Moreover, Aut $S(5, 6, 12) = M_{12}$.

Remark. Lemmas 4 and 5 are concerned with two of the three exceptional situations appearing in the theorem. The third situation occurs when $2n = 12$, and is less interesting. In this case, $\{\bar{x} | x \in [0, 6)\}$ will be identified with $GF(5) \cup \{\infty\}$ as follows:

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
∞	2	4	3	1	0

Then $\bar{O}$ sends $x \to x + 2$ and $\bar{I}$ sends $x \to 2/x$. This identifies $\bar{G}$ with $PGL(2, 5)$. Since $I^6O^5 = (0, 0')$, the transitivity of $\bar{G}$ yields that $|K| = 2^6$. If $k = (2, 2')$ and $l = (3, 3')$, then $k^{-1}O^2k$ and $l^{-1}I^4l$ send $[0, 6)$ to itself and

TABLE II
A Design with Automorphism Group M_{12}

1	5	7	11	0	4	$\xrightarrow{I}$	3	11	8	0	1	9	0	6	11	1	7	8
2	10	9	1	0	8		6	1	7	0	2	5	0	11	1	2	9	7
4	3	5	2	0	7		11	2	9	0	4	10	$\xrightarrow{I}$	0	1	2	4	5	9
8	6	10	4	0	9		1	4	5	0	8	3	0	2	4	8	10	5	
7	11	3	8	0	5		2	8	10	0	7	6	0	4	8	7	3	10	
9	1	6	7	0	10		4	7	3	0	9	11	0	8	7	9	6	3	
5	2	11	9	0	3		8	9	6	0	5	1	0	7	9	5	11	6	
10	4	1	5	0	6		7	5	11	0	10	2	0	9	5	10	1	11	
3	8	2	10	0	11		9	10	1	0	3	4	0	5	10	3	2	1	
6	7	4	3	0	1		5	3	2	0	6	8	0	10	3	6	4	2	
11	9	8	6	0	2		10	6	4	0	11	7	0	3	6	11	8	4	
													1	10	0	3	8	6	
7	6	5	0	10	3		5	7	1	10	8	0	$\xleftarrow{I}$ 2	3	0	6	7	11	
9	11	10	0	3	6		10	9	2	3	7	0	4	6	0	11	9	1	
5	1	3	0	6	11		3	5	4	6	9	0	8	11	0	1	5	2	
10	2	6	0	11	1	$\xleftarrow{I}$	6	10	8	11	5	0	7	1	0	2	10	4	
3	4	11	0	1	2		11	3	7	1	10	0	9	2	0	4	3	8	
6	8	1	0	2	4		1	6	9	2	3	0	5	4	0	8	6	7	
11	7	2	0	4	8		2	11	5	4	6	0	10	8	0	7	11	9	
1	9	4	0	8	7		4	1	10	8	11	0	3	7	0	9	1	5	
2	5	8	0	7	9		8	2	3	7	1	0	6	9	0	5	2	10	
4	10	7	0	9	5		7	4	6	9	2	0	11	5	0	10	4	3	
8	3	9	0	5	10		9	8	11	5	4	0							

induce $PGL(2,5)$ there. Consequently, $\langle I, O\rangle$ is a semi-direct product as asserted in the theorem. (N.B. $-PGL(2,5) \cong S_5$.)

LEMMA 6. (a) *If* $n \equiv 0 \pmod 4$, *then G is in the kernels of the homomorphisms* sgn *and* $\overline{\text{sgn}}$.

(b) *If* $n \equiv 1 \pmod 4$, *then G is in the kernel of* $\overline{\text{sgn}}$.

(c) *If* $n \equiv 3 \pmod 4$, *then G is in the kernel of* $\text{sgn} \cdot \overline{\text{sgn}}$.

Note that parity considerations give no restrictions on G when $n \equiv 2 \pmod 4$. On the other hand, all homomorphisms of B_n in the lemma are onto $\{\pm 1\}$, so that the orders of the groups given in the theorem are upper bounds.

Proof. It suffices to prove that the signs of I, $\bar{I}$, O, and $\bar{O}$ are as in Table III. Since the case of I follows from that of O by replacing n by $n + 1$, we only need to consider the parity of O and $\bar{O}$.

In order to deal with O, we label the cards $0, 1, \ldots, 2n - 1$, so $xO \equiv 2x \pmod{2n - 1}$. Let $x < y$. We need to decide when $xO > yO$. Since $xO = 2x$ or $2x - (2n - 1)$ and $x < y$, the inequality $xO > yO$ holds if and only if $0 \leqslant x \leqslant n - 1$, $n \leqslant y \leqslant 2n - 1$, and $2x > 2y - (2n - 1)$. Thus, for each $x \in [0, n - 1)$ we must restrict y to $[n, x + n)$. The number of pairs (x, y) is then $\sum_{x=0}^{n-1} x = \binom{n}{2}$.

Next, recall that $\overline{xO} = \overline{2x}$ or $\overline{2(n - x) - 1}$. Let $\bar{x} < \bar{y}$ and $\overline{xO} > \overline{yO}$. There are two ways this can happen:

(i) $x, y \geqslant n/2$, in which case $2(n - x) - 1 > 2(n - y) - 1$ holds, or

(ii) $x < n/2$, $y \geqslant n/2$, and $2x > 2(n - y) - 1$, that is, $x + y \geqslant n$.

Set $m = [(n + 1)/2]$. The number of $(\bar{x}, \bar{y})$ in (i) is $\binom{n-m}{2}$. The number in (ii) is obtained by fixing $x \in [0, m)$, and then letting $y \in [n - x, n)$. Thus, the total number of pairs $(\bar{x}, \bar{y})$ is

$$\binom{n-m}{2} + \sum_{x=1}^{m-1} (n - 1 - (n - x) + 1) = \binom{n-m}{2} + \binom{m}{2}.$$

If n is even this is $2\binom{m}{2}$; if n is odd it is $(n - 1)^2/4$. It is now straightforward to check Table III and then deduce Lemma 6. □

Lemma 7 will be used several times. The simple proof is omitted.

LEMMA 7. *Suppose $n \geqslant 3$. Form a graph with vertices the 3-cycles in A_n. Join two 3-cycles when some point of $[0, n)$ is displaced by both of them (i.e., when the corresponding 3-sets are not disjoint). Let H be a subgroup of A_n generated by a connected set of 3-cycles. If each point of $[0, n)$ is displaced by a 3-cycle in H, then $H = A_n$.*

We now begin the main part of the proof of the theorem. Some further notation will be required. If g and h are permutations, and in cycle notation

TABLE III
$(\operatorname{sgn}(g), \operatorname{sgn}(\bar{g}))$ for $g = I$ or O

	$n \pmod 4$							
	0		1		2		3	
I	1	1	−1	1	−1	−1	1	1
O	1	1	1	1	−1	1	−1	−1

h is $\cdots(\ldots, x, y, \ldots)\cdots$, then $h^g = g^{-1}hg$ is $\cdots(\ldots, xg, yg, \ldots)\cdots$. Let z be the element of S_{2n} interchanging x and x' for all $x \in [0, n)$; thus, z has the effect of reversing the order of the deck. Let G^* consist of the elements of G sending $[0, n)$ to itself.

LEMMA 8. *If $G^* \supseteq A_n$ then $|K| \geqslant 2^{n-1}$.*

Proof. By Table III, at least one of the permutations $\bar{I}, \bar{O}$ is even. Let $h \in \langle I, O\rangle$ with $\bar{h}$ even. Let $f \in G^*$ with $\bar{f} = \bar{h}$, and set $k = f^{-1}h$. Then $k \in K - \langle z\rangle$, k fixes $\underline{0}$ and $\underline{0'}$, and k interchanges certain pairs x, x'. Pick any $g \in G^*$ such that $\underline{0}g = \underline{x}$, $\underline{x}g = \underline{0}$ for some such pair x, x', and such that $\underline{y}g = \underline{y}$ whenever $yk = y$. Then $k^g = (x)(x')(00')\cdots$ and $kk^g = (00')(xx')$. Conjugating by elements of G^* produces all permutations $(aa')(bb')$. Thus $|K| \geqslant 2^{n-1}$. □

The argument is easiest for odd n. By Table I we may assume that $n > 3$.

LEMMA 9. *The theorem holds if n is odd.*

Proof. We calculate the following permutations:

$$IO^{-1}: \quad x \to (n-1-x)' \qquad \text{(a cut at the center);}$$

$$I^{-1}O: \begin{cases} 2x \leftrightarrow 2x+1, & \text{if } x < (n-1)/2 \\ n-1 \to (n-1)' & \text{(pairwise adjacent transpositions);} \end{cases}$$

$$I^{-1}O \cdot IO^{-1}: \begin{cases} 2x \to (n-2-2x)', & \text{if } x < (n-1)/2, \\ 2x+1 \to (n-1-2x)', & \text{if } x < (n-1)/2, \\ n-1 \to 0; \end{cases}$$

$$b := (I^{-1}OIO^{-1})^2: \begin{cases} 2x \to 2x+2, & \text{if } x < (n-1)/2, \\ n-1 \to (n-2)', & \\ 2x+1 \to 2x-1, & \text{if } 0 < x < (n-1)/2, \\ 1 \to 0'. & \end{cases}$$

Then

$$b = (0,2,4,\ldots,n-3,n-1,(n-2)',(n-4)',\ldots,1')(0',2',\ldots,1),$$

$$c := b^{O^{-1}} = (0,1,2,\ldots,n-1)(0',1',\ldots,(n-1)'),$$

$$c^2 = (0,2,4,\ldots,n-3,n-1,1,3,\ldots,n-4,n-2)(0',2',\ldots,(n-2)'),$$

$$(c^2)^{I^{-1}O} = (1,3,5,\ldots,n-2,(n-1)',0,2,\ldots,n-5,n-3) \times (1',3',\ldots,(n-3)'),$$

$$v := c^{-2}(c^2)^{I^{-1}O} = (0', n-1, 1)(0, (n-1)', 1'),$$
$$v^{c^{-1}} = ((n-1)', n-2, 0)(n-1, (n-2)', 0'),$$
$$w := (v^{c^{-1}})^{I^{-1}O} = (n-1, n-3, 1)((n-1)', (n-3)', 1').$$

Clearly, c and w belong to G^*. Restricting G^* to $[0, n)$ it is easy to check the connectedness of its set of 3-cycles. Thus, Lemma 7 yields that $G^* \supseteq A_n$. By Lemma 8, $|K| \geqslant 2^{n-1}$.

If $n \equiv 3 \pmod 4$, then $\bar{G}$ contains A_n and the odd permutation $\bar{O}$, so that $\bar{G} = S_n$. Since z is an odd element of S_{2n}, $z \notin G$ by Lemma 6(c). Thus $|K| = 2^{n-1}$, completing the proof in this case.

If $n \equiv 1 \pmod 4$, then $\bar{G} = A_n$ by Lemma 6(b). Thus, there is a $g \in G^*$ with $\bar{g} = \bar{I}$. Clearly, g is even, while I is odd by Table III. Now gI^{-1} is odd and belongs to K. Since K already contains all permutations of the form $(xx')(yy')$ (see the proof of Lemma 8), it follows that $|K| = 2^n$. Then G consists of all permutations in B_n that map to even permutations of S_n. □

The remainder of this section is devoted to the proof of the theorem when n is even. This will be accomplished in a sequence of lemmas.

Notation. $2n = 2^k v$ with $v > 1$ and v odd. (The manner in which $v > 1$ is used can be seen in Lemmas 10 and 12.) Throughout the proof, r will belong to $[1, k)$ (except that $r \in [1, k]$ in Lemma 11).

Lemma 10 determines the result of $O^{-r}I^r$. In the language of cards, the effect of this sequence of shuffles is to reverse the top 2^r cards, and each consecutive group of 2^r cards, in place.

LEMMA 10. *If* $0 \leqslant \alpha < v$ *and* $0 \leqslant \beta < 2^r$, *then* $(2^r\alpha + \beta)O^{-r}I^r = 2^r\alpha + (2^r - 1 - \beta)$ *and* $(2^r\alpha + \beta)'O^{-r}I^r = \{2^r\alpha + (2^r - 1 - \beta)\}'$.

Proof. When $r = 1$, this states that $2\alpha \to 2\alpha + 1$ (for $\beta = 0$) and $2\alpha + 1 \to 2\alpha$ (for $\beta = 1$). Assume inductively that $r > 1$ and $O^{-r+1}I^{r-1}$ behaves as indicated. We must distinguish between the cases $\beta = 2\gamma$ and $\beta = 2\gamma - 1$.

If $\beta = 2\gamma$, then $2^{r-1}\alpha + (2^{r-1} - 1 - \gamma) < 2^{r-1}v \leqslant \frac{1}{2}n$, and

$$\begin{aligned}(2^r\alpha + \beta)O^{-1}O^{-r+1}I^{r-1}I &= (2^{r-1}\alpha + \gamma)O^{-r+1}I^{r-1}I \\ &= \{2^{r-1}\alpha + (2^{r-1} - 1 - \gamma)\}I \\ &= 2\{2^{r-1}\alpha + (2^{r-1} - 1 - \gamma)\} + 1 \\ &= 2^r\alpha + 2^r - 1 - \beta.\end{aligned}$$

Similarly, if $\beta = 2\gamma - 1$, then $2^r\alpha + \beta$ is odd, $2^{r-1}(\alpha + 1) \leqslant \frac{1}{2}n$, and

$$\begin{aligned}
&(2^r\alpha + \beta)O^{-1}O^{-r+1}I^{r-1}I \\
&\quad = \left\{n - \frac{2^r\alpha + \beta + 1}{2}\right\}' O^{-r+1}I^{r-1}I \\
&\quad = \{n - 2^{r-1}(\alpha + 1) + (2^{r-1} - \gamma)\}' O^{-r+1}I^{r-1}I \\
&\quad = \{n - 2^{r-1}(\alpha + 1) + 2^{r-1} - 1 - (2^{r-1} - \gamma)\}' I \\
&\quad = 2n - 2 - 2\{n - 2^{r-1}(\alpha + 1) + \gamma - 1\} \\
&\quad = 2^r(\alpha + 1) - 2\gamma \\
&\quad = 2^r\alpha + 2^r - 1 - \beta. \ \square
\end{aligned}$$

Lemma 11 determines the result of I^rO^{-r}. In the language of cards, the effect of this sequence of shuffles can be described as follows: with the deck on the table, cut off the top $n/2^{r-1}$ cards and place them on the table. Cut off the next $n/2^{r-1}$ cards and place them on the original top group. Continue cutting off packets of size $n/2^{r-1}$, placing them on the cards already cut off, until there are no more cards left.

LEMMA 11. *If* $r \in [1, k]$ *and* $x \in ((i-1)(n/2^{r-1}) - 1, i(n/2^{r-1}) - 1]$ *with* $1 \leqslant i \leqslant 2^{r-1}$, *then*

$$xI^rO^{-r} = \left\{-x - 1 + \frac{n}{2^{r-1}}(2i - 1)\right\}'$$

and $x'I^rO^{-r} = -x - 1 + \dfrac{n}{2^{r-1}}(2i - 1)$.

Proof. The proof is again inductive. If $r = 1$ the lemma states that

$$xIO^{-1} = \{-x - 1 + n\}' \qquad \text{for} \quad x \in (-1, n - 1].$$

Let $r \geqslant 2$. We must distinguish between the cases $x \in [0, \frac{1}{2}n)$ and $x \in [\frac{1}{2}n, n)$.

Let $x \in [0, \frac{1}{2}n)$. Then $xI = 2x+1 \in ((i-1)(n/2^{r-2})-1, i(n/2^{r-2})-1]$ and

$$\begin{aligned}
xII^{r-1}O^{-r+1}O^{-1} &= \left\{-(2x + 1) - 1 + \frac{n}{2^{r-2}}(2i - 1)\right\}' O^{-1} \\
&= \left\{\frac{1}{2}\left[-2x - 2 + \frac{n}{2^{r-2}}(2i - 1)\right]\right\}'.
\end{aligned}$$

Next, let $x \in [\frac{1}{2}n, n)$, so that $xI = (2n - 2x - 2)'$ and

$$-i\frac{n}{2^{r-2}} + 1 \leqslant -(2x+1) < -(i-1)\frac{n}{2^{r-2}} + 1,$$

$$2n - i\frac{n}{2^{r-2}} \leqslant x'I < 2n - (i-1)\frac{n}{2^{r-2}},$$

$$(2^{r-1} - i)\frac{n}{2^{r-2}} - 1 < x'I \leqslant (2^{r-1} - i + 1)\frac{n}{2^{r-2}} - 1.$$

Thus,

$$\begin{aligned} xII^{-r+1}O^{r-1}O^{-1} &= \left[-(2n-2x-2) - 1 + \frac{n}{2^{r-2}}\{2(2^{r-1} - i + 1) - 1\}\right]O^{-1} \\ &= \left\{n - \frac{1}{2}\left[-(2n-2x-2) + \frac{n}{2^{r-2}}(2^r - 2i + 1)\right]\right\}' \\ &= \left\{-x - 1 + \frac{1}{2}\frac{n}{2^{r-2}}(2i-1)\right\}'. \quad \square \end{aligned}$$

LEMMA 12. *Set* $b = (I^kO^{-k} \cdot I^{-1}O)^{-2}$. *Then* b *induces*

$$(0, 2, 4, \ldots, 2v-2)(2v-1, 2v-3, \ldots, 3, 1)$$

on $[0, 2v)$, *and* $(x + 2v)b = xb + 2v$ *whenever* $x, x + 2v \in [0, n)$. *In particular,* b *has order* v.

Proof. Recall that $v = n/2^{k-1}$. Let $x \in [(i-1)v, iv)$. By Lemma 11

$$x'I^kO^{-k} = -x - 1 + v(2i-1) \in [(i-1)v, iv).$$

If x is even, then

$$x'I^kO^{-k} \cdot I^{-1}O = -x + v(2i-1).$$

If x is odd, then

$$x'I^kO^{-k} \cdot I^{-1}O = -x - 2 + v(2i-1).$$

Thus, $x'I^kO^{-k}I^1O \in [(i-1)v, iv)$ unless $-x + v(2i-1) = iv$ and x is even, or $-x - 2 + v(2i-1) = (i-1)v - 1$ and x is odd. Excluding these cases, we find that

$$xb^{-1} = -\{-x + v(2i-1)\} - 2 + v(2i-1) = x - 2 \qquad \text{if } x \text{ is even},$$

$$xb^{-1} = -\{-x - 2 + v(2i-1)\} + v(2i-1) = x + 2 \qquad \text{if } x \text{ is odd}.$$

Finally, if $x = (i-1)v$ is even, then

$$xb^{-1} = -\{-x + v(2i-1)\} - 2 + v(2i+1) = x + (2v-2),$$

while if $x = iv - 1$ is odd, then

$$xb^{-1} = -\{-x - 2 + v(2i-1)\} + v(2i-3) = x - (2v-2). \quad \square$$

LEMMA 13. *Set* $c := b^{O^{-1}}$. *Then* c *induces* $(0, 1, 2, \ldots, v-1)$ *on* $[0, v)$, *and* $(x+v)c = xc + v$ *whenever* $x, x+v \in [0, n)$.

Proof. Since b induces $(2iv, 2iv+2, \ldots, 2iv+2v-2)$ on the even integers in $[2iv, 2iv+2v)$, c acts as indicated on $[0, \frac{1}{2}n)$. Also

$$((2iv+2v-1)', (2iv+2v-3)', \ldots, (2iv+3)', (2iv+1)')^{O^{-1}}$$
$$= (n-iv-v, n-iv-v+1, \ldots, n-iv-2, n-iv-1). \quad \square$$

Notation.

$$h(r) := O^{-r}I^r \qquad \text{for } r \in [1, k),$$
$$h := h(1),$$
$$H = H(1) := \langle b, c, h\rangle \qquad \text{with } b \text{ and } c \text{ as in Lemmas 12 and 13,}$$
$$H(r) := \langle H(r-1), h(r)\rangle \qquad \text{for } r \in (1, k).$$

LEMMA 14. *If* $g \in H(r)$, *then*

$$[0, 2^r v)g = [0, 2^r v) \qquad \textit{and} \qquad (x + 2^r v)g = xg + 2^r v$$

whenever $x, x + 2^r \in [0, n)$. *In particular,* $H(r) \subseteq G^*$.

Proof. This follows immediately from Lemmas 10, 12, and 13. $\square$

LEMMA 15. *If* $v > 3$, *then* H *induces* S_{2v} *on* $[0, 2v)$.

Proof. We will write elements of H as permutations of $[0, 2v)$. Then

$$b = (0, 2, 4, \ldots, 2v-2)(2v-1, \ldots, 3, 1),$$
$$c = (0, 1, 2, \ldots, v-1)(v, v+1, \ldots, 2v-1),$$
$$h = (0\,1)(2\,3)\ldots(v-3, v-2)(v-1, v)(v+1, v+2)\ldots$$
$$\times (2v-4, 2v-3)(2v-2, 2v-1).$$

Note that h is an odd permutation (of $[0, 2v)$).

We will exhibit a 3-cycle. We have

$$h^{c^2} = (2\,3)\cdots(v-1, 0)(1, v+2)(v+3, v+4)\cdots$$
$$\times (2v-2, 2v-1)(v, v+1)$$

so that (since $v \geqslant 5$)

$$d := hh^{c^2} = (0, v+2, v)(1, v-1, v+1).$$

Then

$$\begin{aligned} d^c &= (1, v+3, v+1)(2, 0, v+2), \\ e := d^{d^c} &= (v+2, 2, v)(v+3, v-1, 1), \\ f := e^b &= (v, 4, v-2)(v+5, v+1, 2v-1), \\ e^f &= (v+2, 2, 4)(v+3, v-1, 1), \\ e^{-1}e^f &= (v+2, v, 4). \end{aligned}$$

The connectedness of the set of 3-cycles in H is easily checked. Thus, Lemma 7 applies. □

LEMMA 16. *If $r < k-1$ and $H(r)$ induces at least $A_{2^r v}$ on $[0, 2^r v)$, then $H(r+1)$ induces at least $A_{2^{r+1} v}$ on $[0, 2^{r+1} v)$.*

Proof. We will restrict all permutations to $[0, 2^{r+1}v)$. By hypothesis and Lemma 14, $H(r)$ contains

$$t = (0\,1\,2)(2^r v, 2^r v + 1, 2^r v + 2).$$

By Lemma 10, since $2^r v = 2^r(v-1) + 2^r$ we have

$$\begin{aligned} t^{h(r+1)} = (2^{r+1}-1, 2^{r+1}-2, 2^{r+1}-3)(2^r(v-1) + 2^r - 1, 2^r(v-1) \\ + 2^r - 2, 2^r(v-1) + 2^r - 3) \end{aligned}$$

(if $r = 1$, replace $2^r(v-1) + 2^r - 3$ by $2(v+1) + 2^{r+1} - 1$). Let $g \in H(r)$ fix the last 5 points appearing above in $t^{h(r+1)}$ and send $2^{r+1} - 1$ to 2^{r+1}. Then

$$t^{h(r+1)g}\left(t^{h(r+1)}\right)^{-1} = (2^{r+1}, 2^{r+1}-1, 2^{r+1}-3).$$

Conjugating by elements of $H(r)$, and by $h(r+1)$, we obtain enough 3-cycles to deduce the connectedness of the set of 3-cycles in the action of $H(r+1)$ on $[0, 2^{r+1})$. □

LEMMA 17. *If $v > 3$, then $G^* \supseteq A_n$.*

Proof. This follows from Lemmas 15 and 16 since $H(k-1)$ induces at least A_n on $[0, 2^{k-1}v)$. □

LEMMA 18. *If $v = 3$ and $k \geqslant 4$, then $G^* \supseteq A_n$.*

Proof. Restricting $H(3)$ to $[0, 2^3 \cdot 3)$, we obtain the subgroup of S_{24} generated by the permutations

$$b = (0\,2\,4)(6\,8\,10)(12\,14\,16)(18\,20\,22)(5\,3\,1)(11\,9\,7)(17\,15\,13)(23\,21\,19);$$

$$c = (0\,1\,2)(3\,4\,5)(6\,7\,8)(9\,10\,11)(12\,13\,14)(15\,16\,17)(18\,19\,20)(21\,22\,23);$$

$$h(1): \quad 2x \leftrightarrow 2x + 1;$$

$$h(2): \begin{cases} 4x \leftrightarrow 4x + 3, \\ 4x + 1 \leftrightarrow 4x + 2; \end{cases}$$

$$h(3): \begin{cases} 8x \leftrightarrow 8x + 7, \\ 8x + 1 \leftrightarrow 8x + 6, \\ 8x + 2 \leftrightarrow 8x + 5, \\ 8x + 3 \leftrightarrow 8x + 4. \end{cases}$$

A computer calculation shows that these generate A_{24}, indeed b, c, and $h(3)$ generate A_{24}. (It may be of interest to observe that b, c, and $h(2)$ generate M_{12}.) Now Lemma 16 applies. □

Completion of Proof. We may assume that $2n$ is not a power of 2, and that $2n \neq 12, 24$. By Lemmas 17, 18, and 8, $G^* \supseteq A_n$ and $|K| \geqslant 2^{n-1}$.

If $n \equiv 0 \pmod 4$, then, by Lemma 6(a), $\overline{G} = A_n$ and $|G| \leqslant 2^{n-1}|A_n|$. Thus, (d) holds.

If $n \equiv 2 \pmod 4$, then, by Table III, $\overline{G} = S_n$. Also by Table III, O is odd while $\overline{O}$ is even. Let $g \in G^*$ with $\bar{g} = \overline{O}$. Then gO^{-1} is an odd element of K. As in Lemma 9, the proof of Lemma 8 yields that $|K| = 2^n$, as required. □

3. Some History of the Perfect Shuffle

There are early descriptions of the perfect shuffle in books on cheating at cards. The first description we can find is on p. 91 of the anonymously authored "Whole Art and Mystery of Modern Gaming," Roberts, London, 1726. The earliest American reference to perfect shuffles we can locate is in J. H. Green's book "An Exposure of the Arts and Miseries of Gambling," James, Cincinnati, 1843. On p. 195 he described a method of cheating at the game of Faro which used the perfect shuffle, calling it "running in the cards." Green remarked that the method was a recent invention. The perfect shuffle is currently called the Faro shuffle in magic circles. It is still widely used as a method of cheating at card games such as gin rummy and poker. A detailed description of several uses of the perfect shuffle for cheating at Faro can be found in the anonymously authored book "A Grand Expose of the Science of Gambling" Brady, New York, 1860. An illustrated description of the technique is on pp. 204–205 of J. N. Maskelyne's book "Sharps and Flats," Longmans Green and Co., London, 1894.

The shuffle was introduced to magicians in a brief note in C. T. Jordan's classic "Thirty Card Mysteries," published by the author in Pengrove, Calif., 1919. In a trick called the Full Hand, on pp. 17–19, he used the principle that a 16 card packet out shuffled 4 times returned to its original order. He mentioned that 5 out shuffles suffice for 32 cards and that T. Nelson Downs, a famous American manipulator, could do similar things with 52 cards.

It is through Downs that we have any record of a skillful early practioner of the perfect shuffle: Fred Black, a rancher from Thedford, Nebraska. Black worked out the mathematics of repeated out shuffles of 52 cards in some detail. Downs reported meetings with Black in 1924. These letters are reprinted in the magic journal, *The Linking Ring*, April (1971), 53–83 and May (1971), 67–68; 72–73. Dai Vernon knew Black and said that he used to practice shuffling on horseback. The charts Black worked out depicting some of the group structure of out shuffles appeared first in Hugard and Braue's "Expert Card Technique," Chap. 16. These charts record facts like: cards 18 and 35 repeatedly interchange during repeated out shuffles; the deck breaks up into groups: top, bottom, {18, 35}, 6 "belts" of 8 cards which are permuted among themselves, etc.

The modern era for perfect shuffles in magic begins in 1957 when J. Russell Duck, a Pennsylvania policeman, published the basic central symmetry principle, calling it "stay-stack", in the first issue (Feb. 1957) of the privately published journal *Cardiste*. At about the same time, Alex Elmsley, a computer specialist living in London, began to publish a series of tricks based on the perfect shuffle. In the privately published card magazine *Ibidem* (No. 11, Sept. 1957), he established the binary procedure for bringing the top card to any position (Lemma 2). In a series of articles in the English magic journal *Pentagram* **11** (1957), he set out the basic mathematics for decks of general size, discovering in particular the importance of the order of $2 \bmod (2n \pm 1)$, and the connection with Fermat's little theorem.

While many new tricks based on Faro shuffles have appeared in the magic literature in recent years, few new properties have emerged. (Our theorem, in a sense, explains this.) A scholarly manuscript by Ronald Wohl, a Swiss chemist, completed in the early 1960s has recently been published, in part, in *Ibidem*, No. 36. In two books, "Faro Fantasy" and "More Faro Fantasy," Paul Swinford discovered that with a deck of 2^k cards, the shuffle sequence (in Lemma 2) that brings card x to position y also brings the card at y to position x. Swinford (private communication) also discovered the method for bringing a card at x to position y for 2^k cards. There are a large number of recent articles on the Faro shuffle. Two excellent books by Edward Marlo, "The Faro Shuffle" and "Faro Notes," Ireland Magic Company, Chicago, are currently sold in magic shops.

TABLE IV
Cycle and Type for Out Shuffles of 64 Cards

Cycle	*Type*
(0)	(0)
(1, 2, 4, 8, 16, 32)	(000001)
(3, 6, 12, 24, 48, 33)	(000011)
(5, 10, 20, 40, 17, 34)	(000101)
(7, 14, 28, 56, 49, 35)	(000111)
(9, 18, 36)	(001)
(11, 22, 44, 25, 50, 37)	(001011)
(13, 26, 52, 41, 19, 38)	(001101)
(15, 30, 60, 57, 51, 40)	(001111)
(21, 44)	(011)
(23, 46, 29, 58, 43)	(010111)
(27, 54, 45)	(011)
(31, 62, 61, 59, 55, 47)	(100000)
(63)	(1)

There has been some mathematical work on perfect shuffles. P. Levy wrote a sequence of papers on them in 1940–1950. These papers (Levy [13–18]) are together in Vol. 6 of Levy's collected works. Levy's motivation for working on these shuffles is charmingly described in his autobiography [19, pp. 151–153]. Since Levy's work seems unknown, a brief description is presented. Throughout, a deck of size $2n$ is assumed. We give results for out shuffles. Levy defined the type of a cycle in the cycle decomposition of an out shuffle as follows: suppose a card at position j_1 goes through positions $j_1, j_2, \ldots, j_\sigma$ in successive out shuffles. The *type* of the cycle $(j_1, j_2, \ldots, j_\sigma)$ is a binary vector of length σ with a zero in the ith position if and only if $0 \leqslant j_i \leqslant n$. Table IV lists the cycle and type decomposition for a deck of 64 cards. Levy proved that all cycles have distinct types. When $n = 2^k$ he showed that all types occur if the following conventions are made: two types that differ by a cyclic shift are equivalent. Call a type *imprimitive* if it is made up of repetitions of a single shorter type. (For 64 cards, (0 0 0 0 0 0) (0 0 1 0 0 1) (0 1 0 1 0 1) (1 1 0 1 1 0) (1 1 1 1 1 1) are imprimitive.)

Only the shorter types appear for an imprimitive type. F. Leighton has pointed out that the type result just stated is equivalent to the representation of an out shuffle as a shift operating on Z_2^k, as in the proof of Lemma 4.

A primitive type is "born" at k_0 if it occurs in a deck of k_0 cards and for no smaller deck. Levy showed that if a type is born at k_0, then it appears in a deck of size k if and only if $k = k_0 + 2(k_0 - 1)j$, $j = 0, 1, 2, \ldots$. For example, since a 2-cycle appears for the first time with $k_0 = 4$ cards it follows that decks of size $k = 4 + 6j$ have 2-cycles. Levy proved that for a fixed k, all the new born types are of the same length σ. This σ is the order of 2 (mod $k - 1$). Levy gave a number of other results.

Golomb [9] considered the group generated by out shuffles and cuts. He showed that these operations generate all permutations. He also gave results for a deck of size $2n - 1$. One implication of his results is that in and out shuffles of an odd-sized deck generate a very small group. (Here, in and out shuffles correspond to the two ways of cutting a deck into two parts of size n and $n - 1$. The out shuffle leaves the top card on top, while the in shuffle leaves the bottom card on bottom.)

THEOREM. *The order of the shuffle group for a deck of* $2n - 1$ *cards is* $(2n - 1) \times$ *order of* 2 mod$(2n - 1)$.

Proof. Let c be the operation of cutting the top card to the bottom. It is easy to see that an out shuffle followed by c is the same as an in shuffle. It follows that $\langle O, I \rangle = \langle O, c \rangle$. The order of the latter group was shown to be $(2n - 1) \times$ order of 2 (mod$(2n - 1)$) by Golomb. □

In fact, if the cards are labeled using $[0, 2n - 1)$, then $xO \equiv 2x \pmod{2n - 1}$, $xI \equiv 2x + 1 \pmod{2n - 1}$, and the cut c is given by $xc \equiv x + 1 \pmod{2n - 1}$. The order of $\langle O, c \rangle$ is easily found using the identity $c^O = c^2$ observed by Golomb. In terms of O and $I = Oc$ this asserts that $I^O = (O^{-1})^{I^{-1}}$. The magical properties of perfect shuffles of odd-sized decks are discussed at length in Gardner [8, Chap. 10].

4. Applications of Perfect Shuffles to Parallel Processing Algorithms

Both types of perfect shuffles and their combinations have been applied to computer algorithms. Some references are Stone [25], Schwartz [23], and Chen *et al.* [4]. For a simple example, due to Stone, consider computing the transpose of a $2^m \times 2^m$ matrix. Suppose that the matrix is stored in a 2^{2m} linear array in row major order. For a 4×4 matrix this is $a_{00}a_{01}a_{02}a_{03}a_{10}a_{11}a_{12}a_{13}a_{20}a_{21}a_{22}a_{23}a_{30}a_{31}a_{32}a_{33}$. It is easy to verify that

after m out shuffles the array is in column major order, and so transposed. In the 4×4 example this is $a_{00}a_{10}a_{20}a_{30}a_{11}a_{21}a_{31}a_{12}a_{32}a_{03}a_{13}a_{23}a_{33}$.

Out shuffles are performed by network connection patterns like the example in Fig. 1 in which 2 sets of 8 registers are connected. Often an out shuffle connection is combined with an array of simple processors (Fig. 2). If the processors P take two input numbers and output their sum (Fig. 3) then, after m iterations of a network with 2^m registers, all registers will contain the sum $a_0 + a_1 + \cdots + a_{2^m-1}$. If the processors output other

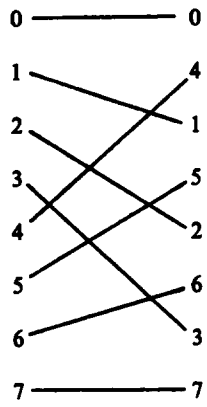

FIGURE 1

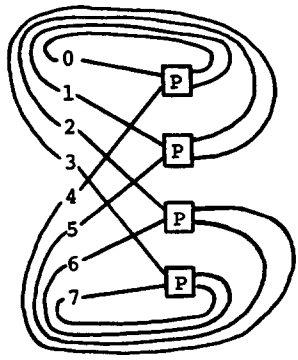

FIGURE 2

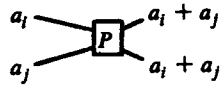

FIGURE 3

suitably chosen linear combinations the result of m iterations is the discrete Fourier transform $\Sigma a_j \omega^{jk}$. In a more complex application the processors output the sorted pair (a_i, a_j). This yields an algorithm that sorts 2^m numbers in $O(m^2)$ iterations. See Brock *et al.* [3] for further discussion.

It should be emphasized that these applications mostly amount to the "out" part of the proof of Lemma 4. Namely, when O is used on a deck of size 2^m it cyclically shifts the digits in the binary expansion of each integer in $[0, 2^m)$.

As a simple new example, we mention the fact that *an array of* 2^m *numbers is brought into reverse order by m in shuffles*. Other length arrays may also be reversed; for length 52, 26 in shuffles suffice. In general, an array of length $2n$ reverses after j in shuffles, where j is the smallest exponent such that $2^j \equiv -1 (\mathrm{mod}\, 2n + 1)$. In shuffles cannot always be called upon to reverse an array of length $2n$. For example, if $2n = 2^m - 2$, the order of 2 $(\mathrm{mod}\, 2n + 1)$ is m and $2^j \not\equiv -1 (\mathrm{mod}\, 2n + 1)$ for any j. A simple corollary of the main theorem is that *an array of length* $2n$ *can be reversed by some combination of in and out shuffles if and only if* $n \equiv 0, 1,$ *or* $2 (\mathrm{mod}\, 4)$. Indeed, if z denotes the permutation reversing the position of $2n$ symbols, $\mathrm{sgn}\, z = (-1)^n$, $\mathrm{sgn}\, \bar{z} = 1$, now apply Lemma 5 and the theorem. As an example, if $2n = 10$, the sequence $IOOIOOOOO$ yields z. We do not know a simple algorithm for determining a minimal length sequence for general n.

5. Generalizations and Variations

In and out shuffles are related to the so-called "milk" and "Monge" shuffles. The milk shuffle can be described as a permutation on m cards labeled $0, 1, \ldots, m - 1$ as follows. The card labeled j (and initially in position j) is moved to position $|2j|$, where $|x|$ denotes the unique y, $0 \leqslant y \leqslant m$, such that $y \equiv \pm x (\mathrm{mod}\, 2m - 1)$. Thus, after one milk shuffle, the deck now has the order $0, m - 1, 1, m - 2, 2, \ldots$. This permutation is easily performed on a deck of cards. Remove, or "milk," the cards at top and bottom simultaneously and place them on the table. Then milk off the second pair from the top and bottom and place them on top of the first removed pair. Continue this process until no cards remain. Basic properties of the milk shuffle were given by Levy in the papers cited in the bibliography. Levy [18] showed that the results he proved for milk shuffles had easy translations into corresponding results for out shuffles. A useful connection between the two shuffles is the following observation due to John Conway. The permutation of the pairs $\bar{x}$ in an out shuffle of $2m$ cards is just a milk shuffle of the m symbols $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{m-1}$. The inverse of the milk shuffle was actually analyzed by Monge in 1773 (see Ball and Coxeter [1]). In fact, there are two types of "Monge" shuffles, which we will call the

"up" shuffle and the "down" shuffle. For the up shuffle, successive cards are removed from the top of the deck and placed alternatively on the top and the bottom of the new stack (with the second card being placed on top of the first). For the down shuffle, the same procedure is followed except that the second card is placed below the first. In particular the order of a milk shuffle of m cards is the order of an out shuffle of $2m$ cards: the order of 2 (mod $2m - 1$). Symbolically, for a deck of m cards, the up shuffle sends a card originally in position j to position $[m/2] + (-1)^j[(j + 1)/2]$. Note that a down shuffle is actually just an up shuffle followed by a "reversal" shuffle z, i.e., $z(j) = m - 1 - j$. It follows from what we have noted that the group $\langle u, d \rangle$ of permutations generated by up and down shuffles on m cards is exactly $\langle \bar{I}, \bar{O} \rangle$ acting on (pairs of) $2m$ cards. In particular, since $\langle u, d \rangle = \langle u, z \rangle$, it follows that for $m \equiv 2 \pmod 4$, $\langle u, z \rangle \cong S_m$ while for $m = 12$, $\langle u, z \rangle \cong M_{12}$. Borcherds *et al.* [2] have used this fact in order to relate two different bases for the Leech lattice.

Levy also mentioned a curious connection between the milk shuffle and the down and under shuffle. This shuffle successively places the top card on the table, the next card under the deck, the next card on (top of the card on) the table, and so on. Let E be the set of integers with the property that the milk shuffle and the down and under shuffle have the same cycle structure (and in particular the same order). Levy showed that $n \in E$ if and only if $2n - 1$ divides a number of the form $2^r + 1$. For example, a milk shuffle with 5 cards labeled 01234 gives the permutation

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 3 & 1. \end{matrix}$$

A down and under shuffle gives the permutation

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 4 & 1 & 3 & 2. \end{matrix}$$

Both permutations have one 3-cycle and two fixed points, and $2n - 1 = 9$ which divides $2^3 + 1$. A. M. Odlyzko has shown that E is small in the sense of density: the number of elements in E smaller than x is asymptotic to $cx/(\log x)^{2/3}$ for an explicit constant c. The down and under shuffle is thoroughly studied under the name of the Josephus permutation (see Herstein and Kaplansky [11]). The milk shuffle is described and applied in early books on card cheating. For example, the anonymously authored book "Whole Art and Mystery of Modern Gaming" (London, 1726) contains a description of several methods of cheating at the card game of Faro that make use of milk shuffles.

A simple way to achieve an inverse in or out shuffle is to deal a deck of cards into two face-up piles alternatively. Place one pile on the other, and

turn the deck face down. This suggests a generalized perfect out shuffle: for a deck consisting of $a \cdot b$ cards, deal a face-up piles and gather the piles so that the original top card remains on top. This shuffling operation arises naturally in circuit applications such as the final shuffling in the Cooley–Tukey algorithms for the discrete Fourier transform. Davio [6] contains a nice discussion of this and other examples. One application involves the noncommutativity of tensor products. If the permutation matrix of the generalized out shuffle is denoted $S_{a,b}$ and if m_1 and m_0 are (r_1, c_1) and (r_0, c_0) matrices, then Davio [6] showed that

$$m_1 \otimes m_0 = S_{r_0, r_1}(m_0 \otimes m_1)S_{c_1, c_0}.$$

Morris and Hartwig [22] have determined properties of generalized out shuffles and generalized out shuffles and cuts; they also proved a special case of the above formula (when $r_1 = c_1$ and $r_0 = c_0$). We observe that it is also possible to define generalized in shuffles by picking up the piles in the opposite order. Both generalized in and out shuffles preserve central symmetry; it would be interesting to know what group these generate. Going further, if $a \cdot b$ cards are dealt into a piles with b cards in each pile, there are $a!$ possible ways of picking up the piles, and this leads to more questions of the same sort.

ACKNOWLEDGMENTS

This paper makes heavy use of computational results generated by Eric Hamilton in a course at Stanford taught by Don Knuth. The calculations leading to M_{12} and a crucial computer check required in the proof of the main theorem were carried out by Lyle Ramshaw at Xerox PARC. Rob Calderbank and Neil Sloane provided the first corroboration that for $n = 12$, $\overline{G} = M_{12}$. A. M. Odlyzko produced the difficult estimate in Section 5. We thank them all for their help.

REFERENCES

1. W. W. R. BALL AND H. M. S. COXETER, "*Mathematical Recreations and Essays*," 12th ed., University of Toronto Press, Buffalo, 1974.
2. R. BORCHERDS, J. H. CONWAY, L. QUEEN, AND N. J. A. SLOANE, "A Monster Lie Algebra?" Technical Report, Bell Laboratories, Murray Hill, N.J., 1982.
3. H. K. BROCK, B. J. BROOKS, AND F. SULLIVAN, Diamond, a sorting method for vector machines, *BIT* **21** (1981), 142–152.
4. P. Y. CHEN, D. H. LAWRIE, P. C. YEW, AND D. A. PODERA, Interconnection networks using shuffles, *Computer*, December (1981), 55–64.
5. H. M. S. COXETER, "Regular Polytopes," Methuen, London, 1948.
6. M. DAVIO, Kronecker products and shuffle algebra, *IEEE Trans. Comput.* **C-30** (1981), 116–125.

7. M. FURST, J. HOPCROFT, AND E. LUKS, Polynomial-time algorithms for permutation groups, *in* "Proc. 21st FOCS," pp. 36–41, 1980.
8. M. GARDNER, "Mathematical Carnival," Knopf, New York, 1975.
9. S. W. GOLOMB, Permutations by cutting and shuffling, *SIAM Rev.* **3** (1961), 293–297.
10. R. E. HARTWIG AND S. B. MORRIS, The universal flip matrix and the generalized Faro shuffle, *Pacific J. Math.* **58** (1975), 445–455.
11. I. N. HERSTEIN AND I. KAPLANSKY, "Matters Mathematical," Harper & Row, New York, 1974.
12. D. KLEITMAN, F. LEIGHTON, M. LEPLEY, AND G. MILLER, "New Layouts for the Shuffle–Exchange Graph," Technical report, Applied Mathematics Department, M.I.T., Cambridge, Mass., 1980.
13. P. LEVY, Étude d'une classe de permutations, *C. R. Acad. Sci.* **227** (1948), 422–423.
14. P. LEVY, Étude d'une nouvelle classe de permutations, *C. R. Acad. Sci.*, **227** (1948), 578–579.
15. P. LEVY, Sur deux classes de permutations, *C. R. Acad. Sci.* **228** (1949), 1089–1090.
16. P. LEVY, Un problem de la théorie des permutations, *in* "Conf. École Polyt.," May 24, 1949.
17. P. LEVY, Sur une classe remarquable de permutations, *Bull. Acad. Roy. Belgique* **2** (1949), 361–377.
18. P. LEVY, Sur quelque classes de permutations, *Compositio Math.* **8** (1950), 1–48.
19. P. LEVY, "Quelques aspects de la pensée d'un mathématician," Blanchard, Paris, 1970.
20. S. B. MORRIS, "Permutations by Cutting and Shuffling—A Generalization to Q-Dimensions," Ph.D. dissertation, Department of Mathematics, Duke University. Published under the same title by Micky Hades, Box 476, Calgary, Alberta, Canada.
21. S. B. MORRIS, The basic mathematics of the Faro shuffle, *Pi Mu Epsilon J.* **6** (1975), 85–92.
22. S. B. MORRIS AND R. E. HARTWIG, The generalized Faro shuffle, *Discrete Math.* **15** (1976), 333–346.
23. J. T. SCHWARTZ, Ultracomputers, *ACM Trans. Program. Language Systems* **2** (1980), 484–521.
24. C. C. SIMS, Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra," Proc. Conf., Oxford, 1967 (John Leech, Ed.), pp. 169–183, Pergamon, Oxford, 1970.
25. H. S. STONE, Parallel processing with the perfect shuffle, *IEEE Trans. Comput.* **2** (1971), 153–161.
26. J. V. USPENSKY AND M. A. HEASLET, "Elementary Number Theory," McGraw–Hill, New York, 1939.